

# Microsoft

## Exam Questions MS-102

Microsoft 365 Administrator Exam



**NEW QUESTION 1**

- (Exam Topic 1)

You need to meet the Intune requirements for the Windows 10 devices.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Settings to configure in Azure AD:

▼
Device settings
Mobility (MDM and MAM)
Organizational relationships
User settings

Settings to configure in Intune:

▼
Device compliance
Device configuration
Device enrollment
Mobile Device Management Authority

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

References:

<https://docs.microsoft.com/en-us/intune/windows-enroll>

**NEW QUESTION 2**

- (Exam Topic 2)

Which report should the New York office auditors view?

- A. DLP policy matches
- B. DLP false positives and overrides
- C. DLP incidents
- D. Top Senders and Recipients

**Answer:** C

**Explanation:**

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies>

This report also shows policy matches over time, like the policy matches report. However, the policy matches report shows matches at a rule level; for example, if an email matched three different rules, the policy matches report shows three different line items. By contrast, the incidents report shows matches at an item level; for example, if an email matched three different rules, the incidents report shows a single line item for that piece of content. Because the report counts are aggregated differently, the policy matches report is better for identifying matches with specific rules and fine tuning DLP policies. The incidents report is better for identifying specific pieces of content that are problematic for your DLP policies.

**NEW QUESTION 3**

- (Exam Topic 2)

You need to meet the technical requirement for the SharePoint administrator. What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

From the Security & Compliance admin center, perform a search by using:

▼
Audit log
Data governance events
DLP policy matches
eDiscovery

Filter by:

▼
Activity
Detail
Item
User agent

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance>

**NEW QUESTION 4**

- (Exam Topic 3)

You need to create the DLP policy to meet the technical requirements. What should you configure first?

- A. sensitive info types
- B. the Insider risk management settings
- C. the event types
- D. the sensitivity labels

**Answer:** A

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-test-tune-dlp-policy?view=o365-worldwide>

**NEW QUESTION 5**

- (Exam Topic 3)

You need to configure the information governance settings to meet the technical requirements.

Which type of policy should you configure, and how many policies should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Policy type:  

- Label
- Retention
- Auto-labeling

Number of required policies:  

- 1
- 2
- 3

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

Policy type:  

- Label
- Retention
- Auto-labeling

Number of required policies:  

- 1
- 2
- 3

**NEW QUESTION 6**

- (Exam Topic 4)

You are evaluating the required processes for Project1.

You need to recommend which DNS record must be created while adding a domain name for the project. Which DNS record should you recommend?

- A. host (A)
- B. host information
- C. text (TXT)
- D. pointer (PTR)

**Answer:** A

**Explanation:**

When you add a custom domain to Office 365, you need to verify that you own the domain. You can do this by adding either an MX record or a TXT record to the DNS for that domain.

Note:

There are several versions of this question in the exam. The question has two possible correct answers: Text (TXT)

Mail exchanger (MX)

incorrect answer options you may see on the exam include the following: alias (CNAME)

Host (A) host (AAA)

Pointer (PTR) Name Server (NS)  
 host information (HINFO) pointer (PTR)

Reference:

<https://docs.microsoft.com/en-us/office365/admin/get-help-with-domains/create-dns-records-at-any-dns-hosting>

**NEW QUESTION 7**

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription that uses Microsoft Intune. The subscription contains the resources shown in the following table.

Name	Type	Member of
User1	User	Group1
Device1	Device	Group2

User1 is the owner of Device1.

You add Microsoft 365 Apps Windows 10 and later app types to Intune as shown in the following table. On Thursday, you review the results of the app deployments.

Name	Shows in Company Portal	Assignment	Microsoft Office app to install	Day of creation
App1	Yes	Group1 - Required	Word	Monday
App2	Yes	Group2 - Required	Excel	Tuesday
App3	Yes	Group1 - Available	PowerPoint	Wednesday

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Word is installed on Device1.	<input checked="" type="radio"/>	<input type="radio"/>
App3 is displayed in the Company Portal.	<input type="radio"/>	<input type="radio"/>
Excel is installed on Device1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
Word is installed on Device1.	<input checked="" type="radio"/>	<input type="radio"/>
App3 is displayed in the Company Portal.	<input checked="" type="radio"/>	<input type="radio"/>
Excel is installed on Device1.	<input checked="" type="radio"/>	<input type="radio"/>

**NEW QUESTION 8**

- (Exam Topic 5)

You have a Microsoft 365 tenant.

You plan to manage incidents in the tenant by using the Microsoft 365 security center.

Which Microsoft service source will appear on the Incidents page of the Microsoft 365 security center?

- A. Microsoft Defender for CloudUse the
- B. Microsoft Purview
- C. Azure Arc
- D. Microsoft Defender for Identity

Answer: D

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-alerts?view=o365-worldwide>

**NEW QUESTION 9**

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription.

You create an account for a new security administrator named SecAdmin1.

You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint and OneDrive.

Solution: From the Azure Active Directory admin center, you assign SecAdmin1 the Teams Administrator role.  
 Does this meet the goal?

- A. Yes
- B. no

**Answer: B**

**NEW QUESTION 10**

- (Exam Topic 5)

You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

Name	Azure Active Directory (Azure AD) role	Microsoft Store for Business role	Member of
User1	Application administrator	Basic Purchaser	Group1
User2	None	Purchaser	Group2
User3	None	Basic Purchaser	Group3

You perform the following actions:

- > Provision the private store in Microsoft Store for Business.
- > Add an app named App1 to the private store.
- > Set Private store availability for App1 to Specific groups, and then select Group3.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 can install App1 from the private store.	<input type="radio"/>	<input type="radio"/>
User2 can install App1 from the private store.	<input type="radio"/>	<input type="radio"/>
User3 can install App1 from the private store.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Text Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/microsoft-store/app-inventory-management-microsoft-store-for-business#priva>

**NEW QUESTION 10**

- (Exam Topic 5)

HOTSPOT

You have a Microsoft 365 E3 subscription.

You plan to launch Attack simulation training for all users.

Which social engineering technique and training experience will be available? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Social engineering technique:

Training experience:

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Box 1: Credential Harvest

Attack simulation training offers a subset of capabilities to E3 customers as a trial. The trial offering contains the ability to use a Credential Harvest payload and the ability to select 'ISA Phishing' or 'Mass Market Phishing' training experiences. No other capabilities are part of the E3 trial offering.

Note: In Attack simulation training, multiple types of social engineering techniques are available: Credential Harvest Malware Attachment Link to Malware Etc.  
 Box 2: Mass Market Phishing Reference:  
<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training-get-start>

**NEW QUESTION 15**

- (Exam Topic 5)

You have a Microsoft 365 subscription.

You register two applications named App1 and App2 to Azure AD.

You need to ensure that users who connect to App1 require multi-factor authentication (MFA). MFA is required only for App1. What should you do?

- A. From the Microsoft Entra admin center, create a conditional access policy
- B. From the Microsoft 365 admin center, configure the Modern authentication settings.
- C. From the Enterprise applications blade of the Microsoft Entra admin center, configure the Users settings.
- D. From Multi-Factor Authentication, configure the service settings.

**Answer: A**

**Explanation:**

Use Conditional Access policies

If your organization has more granular sign-in security needs, Conditional Access policies can offer you more control. Conditional Access lets you create and define policies that react to sign in events and request additional actions before a user is granted access to an application or service.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authenticati>

**NEW QUESTION 17**

- (Exam Topic 5)

HOTSPOT

You have a Microsoft 365 subscription.

A user named user1@contoso.com was recently provisioned.

You need to use PowerShell to assign a Microsoft Office 365 E3 license to User1. Microsoft Bookings must NOT be enabled.

How should you complete the command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Box 1: Connect-MgGraph

Assign Microsoft 365 licenses to user accounts with PowerShell Use the Microsoft Graph PowerShell SDK

First, connect to your Microsoft 365 tenant.

Assigning and removing licenses for a user requires the User.ReadWrite.All permission scope or one of the other permissions listed in the 'Assign license' Microsoft Graph API reference page.

The Organization.Read.All permission scope is required to read the licenses available in the tenant. Connect-MgGraph -Scopes User.ReadWrite.All, Organization.Read.All

Box 2: Get-MgSubscribedSku

Run the Get-MgSubscribedSku command to view the available licensing plans and the number of available licenses in each plan in your organization. The number of available licenses in each plan is ActiveUnits - WarningUnits - ConsumedUnits.

Box 3: Set-MgUserLicense

Assigning licenses to user accounts

To assign a license to a user, use the following command in PowerShell.

```
Set-MgUserLicense -UserId $userUPN -AddLicenses @{$Skuld = "<Skuld>"} -RemoveLicenses @() This example assigns a license from the SPE_E5 (Microsoft 365 E5) licensing plan to the unlicensed user belindan@litwareinc.com:
$e5Sku = Get-MgSubscribedSku -All | Where SkuPartNumber -eq 'SPE_E5'
Set-MgUserLicense -UserId "belindan@litwareinc.com" -AddLicenses @{$Skuld = $e5Sku.Skuld}
-RemoveLicenses @()
Reference:
https://learn.microsoft.com/en-us/microsoft-365/enterprise/assign-licenses-to-user-accounts-with-microsoft-365
```

**NEW QUESTION 20**

- (Exam Topic 5)

You have a Microsoft 365 subscription that uses Security & Compliance retention policies. You implement a preservation lock on a retention policy that is assigned to all executive users.

Which two actions can you perform on the retention policy? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point?

- A. Add locations to the policy
- B. Reduce the duration of policy
- C. Remove locations from the policy
- D. Extend the duration of the policy
- E. Disable the policy

**Answer:** AD

**NEW QUESTION 23**

- (Exam Topic 5)

You have a Microsoft 365 subscription that contains three groups named All users, Sales team, and Office users, and two users shown in the following table.

Name	Member of
User1	All users, Sales team
User2	All users, Office users

In Microsoft Endpoint Manager, you have the Policies for Office apps settings shown in the following exhibit.



The policies use the settings shown in the following table.

Policy	Default Shared Folder Location	Default Office Theme
All users	https://sharepoint.contoso.com/addins_all_users	Colorful
Office Users Policy	https://sharepoint.contoso.com/addins_office_users	White
Sales Team Policy	https://sharepoint.contoso.com/addins_sales_team_users_	Dark Gray

What is the default share folder location for User1 and the default Office theme for User2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

The default shared folder location for User1 is:

https://sharepoint.contoso.com/addins\_all\_users

https://sharepoint.contoso.com/addins\_office\_users

https://sharepoint.contoso.com/addins\_sales\_team\_users\_

The default Office theme for User 2 is:

Colorful

Dark Gray

White

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Table Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/deployoffice/overview-office-cloud-policy-service>

**NEW QUESTION 25**

- (Exam Topic 5)

You have an Azure AD tenant that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

Your company uses Microsoft Defender for Endpoint. Microsoft Defender for Endpoint contains the roles shown in the following table.

Name	Permission	Assigned user group
Microsoft Defender for Endpoint administrator (default)	View data, Alerts investigation, Active remediation actions, Manage security settings	Group3
Role1	View data, Alerts investigation	Group1
Role2	View data	Group2

Microsoft Defender for Endpoint contains the device groups shown in the following table.

Rank	Device group	Device name	User access
1	ATP1	Device1	Group1
Last	Ungrouped devices (default)	Device2	Group2

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE; Each correct selection is worth one point.

**Answer Area**

Statements	Yes	No
User1 can run an antivirus scan on Device2.	<input type="radio"/>	<input type="radio"/>
User2 can collect an investigation package from Device2.	<input type="radio"/>	<input type="radio"/>
User3 can isolate Device1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

**Answer Area**

Statements	Yes	No
User1 can run an antivirus scan on Device2.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can collect an investigation package from Device2.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can isolate Device1.	<input checked="" type="radio"/>	<input type="radio"/>

**NEW QUESTION 28**

- (Exam Topic 5)

HOTSPOT

You have a Microsoft 365 E5 subscription.

You need to implement identity protection. The solution must meet the following requirements:

- > Identify when a user's credentials are compromised and shared on the dark web.
- > Provide users that have compromised credentials with the ability to self-remediate. What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

**Answer Area**

To identify when users have compromised credentials, configure:

A registration policy
A sign-in risk policy
A user risk policy
A multifactor authentication registration policy

To enable self-remediation, select:

Generate a temporary password
Require multi-factor authentication
Require password change

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: A user risk policy

Identify when a user's credentials are compromised and shared on the dark web. User risk-based Conditional Access policy Identity Protection analyzes signals about user accounts and calculates a risk score based on the probability that the user has been compromised. If a user has risky sign-in behavior, or their credentials have been leaked, Identity Protection will use these signals to calculate the user risk level. Administrators can configure user risk-based Conditional Access policies to enforce access controls based on user risk, including requirements such as:

Block access

Allow access but require a secure password change.

A secure password change will remediate the user risk and close the risky user event to prevent unnecessary noise for administrators.

Box 2: Require password change

Provide users that have compromised credentials with the ability to self-remediate.

A secure password change will remediate the user risk and close the risky user event to prevent unnecessary noise for administrators

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies#>

**NEW QUESTION 31**

- (Exam Topic 5)

You have a Microsoft 365 E5 tenant.

You need to evaluate compliance with European Union privacy regulations for customer data. What should you do in the Microsoft 365 compliance center?

- A. Create a Data Subject Request (DSR)
- B. Create a data loss prevention (DLP) policy for General Data Protection Regulation (GDPR) data
- C. Create an assessment based on the EU GDPR assessment template
- D. Create an assessment based on the Data Protection Baseline assessment template

**Answer:** C

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-action-plan>

**NEW QUESTION 32**

- (Exam Topic 5)

**HOTSPOT**

You have a Microsoft 365 tenant.

You need to create a custom Compliance Manager assessment template.

Which application should you use to create the template, and in which file format should the template be saved? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Application:

Microsoft Excel
Microsoft Forms
Microsoft Word
Visual Studio Code

File format:

csv
dbx
docx
dotx
json
xlsx
xltx

- A. Mastered

B. Not Mastered

**Answer:** A

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-templates-create?view=o365>

**NEW QUESTION 33**

- (Exam Topic 5)

HOTSPOT

You have an Azure AD tenant that contains the administrative units shown in the following table.

Name	Members
AU1	User1, User2
AU2	User3

You have the following users:

- > A user named User1 that is assigned the Password Administrator for AU1 and AU2.
- > A user named User2 that is assigned the User Administrator for AU1.
- > A user named User3 that is assigned the User Administrator for the tenant.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

**Answer Area**

Statements	Yes	No
User1 can reset the password of User3.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
User2 can update the display name of User1.	<input type="checkbox"/>	<input type="checkbox"/>
User1 can reset the password of User2.	<input type="checkbox"/>	<input type="checkbox"/>

A. Mastered  
 B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: No

User1 is assigned the Password Administrator for AU1 and AU2. User3 is in AU2. User3 is User Administrator.

Password administrators cannot reset User Administrators passwords. Note: Password Administrator

Users with this role have limited ability to manage passwords. This role does not grant the ability to manage service requests or monitor service health. Whether a Password Administrator can reset a user's password depends on the role the user is assigned.

Role that password can be reset	Password Admin	Helpdesk Admin	Auth Admin	User Admin	Privileged Auth Admin	Global Admin
User Admin	<input type="checkbox"/>			✓	✓	✓
Usage Summary Reports Reader		✓	✓	✓	✓	✓

Box 2: Yes

Box 3: No

User1 is assigned the Password Administrator for AU1 and AU2. User2 is in AU1. User2 is User Administrator.

Password administrators cannot reset User Administrators passwords.

Note: User Administrator

Can manage all aspects of users and groups, including resetting passwords for limited admins. Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#who-can-reset-passwords> <https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference>

**NEW QUESTION 38**

- (Exam Topic 5)

You have a Microsoft 365 E5 tenant that contains the devices shown in the following table.

Name	Windows 10 edition	Azure Active Directory (Azure AD)	Mobile device management (MDM) enrollment
Device1	Windows 10 Pro	Registered	Microsoft Intune
Device2	Windows 10 Enterprise	Joined	Microsoft Intune
Device3	Windows 10 Pro	Joined	Not enrolled
Device4	Windows 10 Enterprise	Registered	Microsoft Intune
Device5	Windows 10 Enterprise	Joined	Not enrolled

You add custom apps to the private store in Microsoft Store Business.

You plan to create a policy to show only the private store in Microsoft Store for Business. To which devices can the policy be applied?

- A. Device2 only
- B. Device1 and Device3 only
- C. Device2 and Device4 only
- D. Device2, Device3, and Device5 only
- E. Device1, Device2, Device3, Device4, and Device5

**Answer:** C

**NEW QUESTION 43**

- (Exam Topic 5)

You have a Microsoft 365 tenant.

You need to retain Azure Active Directory (Azure AD) audit logs for two years. Administrators must be able to query the audit log information by using the Azure Active Directory admin center.

What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

**Answer Area**

Save the audit logs to:

Azure Active Directory admin center blade to use to view the saved audit logs:

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

Save the audit logs to: Azure Log Analytics

Azure Active Directory admin center blade to use to view the saved audit logs: Audit logs

**NEW QUESTION 45**

- (Exam Topic 5)

You have a Microsoft 365 subscription.

You have an Azure AD tenant that contains the users shown in the following table.

Name	Role
User1	Security Administrator
User2	Global Administrator
User3	Service Support Administrator

You configure Tenant properties as shown in the following exhibit.

Technical contact

Global privacy contact

Privacy statement URL

Which users will be contacted by Microsoft if the tenant experiences a data breach?

- A. User1 only
- B. User2 only
- C. User3 only
- D. User1 and User2 only
- E. User2 and User3 only

**Answer:** B

**Explanation:**

Microsoft 365 is committed to notifying customers within 72 hours of breach declaration. The customer's tenant administrator will be notified.

Reference:

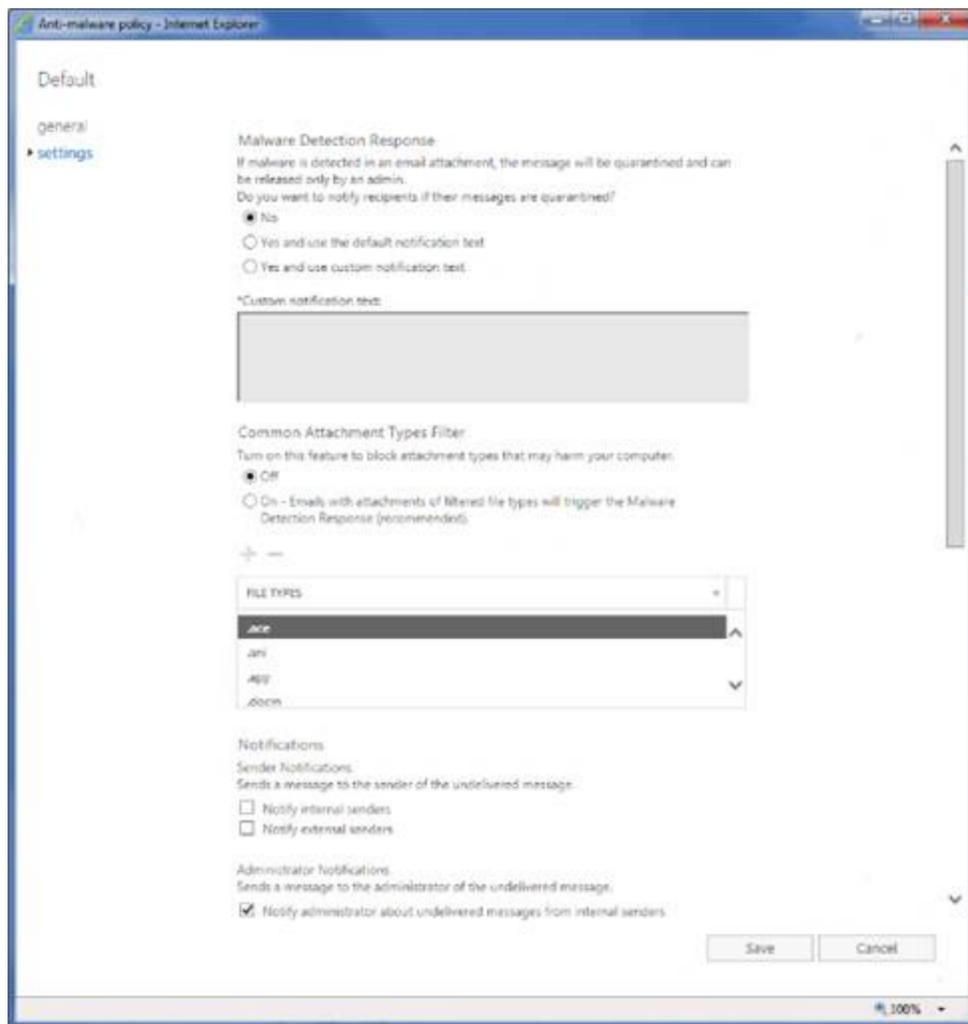
<https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-breach-office365>

**NEW QUESTION 48**

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription that contains a user named User1.

The subscription has a single anti-malware policy as shown in the following exhibit.



An email message that contains text and two attachments is sent to User1. One attachment is infected with malware. How will the email message and the attachments be processed?

- A. Both attachments will be remove
- B. The email message will be quarantined, and Used will receive an email message without any attachments and an email message that includes the following text: 'Malware was removed.'
- C. The email message will be quarantined, and the message will remain undelivered.
- D. Both attachments will be remove
- E. The email message will be quarantined, and User1 will receive a copy of the message containing the original text and a new attachment that includes the following text: 'Malware was removed.'
- F. The malware-infected attachment will be remove
- G. The email message will be quarantined, and User1 will receive a copy of the message containing only the uninfected attachment.

**Answer: C**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-malware-protection?view=o36>

**NEW QUESTION 53**

- (Exam Topic 5)

You have a Microsoft 365 F5 subscription.

You plan to deploy 100 new Windows 10 devices.

You need to order the appropriate version of Windows 10 for the new devices. The version must Meet the following requirements.

Be serviced for a minimum of 24 moths.

Support Microsoft Application Virtualization (App-V) Which version should you identify?

- A. Window 10 Pro, version 1909
- B. Window 10 Pro, version 2004
- C. Window 10 Pro, version 1909
- D. Window 10 Enterprise, version 2004

**Answer: D**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/windows/release-health/release-information> <https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-supported-configurations>

**NEW QUESTION 58**

- (Exam Topic 5)

HOTSPOT

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of	Multi-factor authentication (MFA) method registered
User1	Group1	Microsoft Authenticator app (push notification)
User2	Group2	Microsoft Authenticator app (push notification)
User3	Group1	None

You configure the Microsoft Authenticator authentication method policy to enable passwordless authentication as shown in the following exhibit.



Both User1 and User2 report that they are NOT prompted for passwordless sign-in in the Microsoft Authenticator app. For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

**Answer Area**

**Statements**

	Yes	No
User1 will be prompted for passwordless authentication once User1 sets up phone sign-in in the Microsoft Authenticator app.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
User2 will be prompted for passwordless authentication once User2 sets up phone sign-in in the Microsoft Authenticator app.	<input type="checkbox"/>	<input type="checkbox"/>
User3 can use passwordless authentication without further action.	<input type="checkbox"/>	<input type="checkbox"/>

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Box 1: Yes

User1 is member of Group1.

User1 has MFA registered method of Microsoft Authenticator app (push notification)

The Microsoft Authenticator authentication method policy is configured for Group1, registration is optional, authentication method is any.

Note: Microsoft Authenticator can be used to sign in to any Azure AD account without using a password. Microsoft Authenticator uses key-based authentication to enable a user credential that is tied to a device, where the device uses a PIN or biometric. Windows Hello for Business uses a similar technology.

This authentication technology can be used on any device platform, including mobile. This technology can also be used with any app or website that integrates with Microsoft Authentication Libraries.

Box 2: No

User2 is member of Group2.

The Microsoft Authenticator authentication method policy is configured for Group1, not for Group2. Box 3: No

User3 is member of Group1.

User3 has no MFA method registered.

User3 must choose an authentication method.

Note: Enable passwordless phone sign-in authentication methods

Azure AD lets you choose which authentication methods can be used during the sign-in process. Users then register for the methods they'd like to use.

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-passwordless-phon>

**NEW QUESTION 62**

- (Exam Topic 5)

You have a Microsoft 365 E5 tenant.

You plan to deploy a monitoring solution that meets the following requirements:

- > Captures Microsoft Teams channel messages that contain threatening or violent language.
- > Alerts a reviewer when a threatening or violent message is identified.

What should you include in the solution?

- A. Data Subject Requests (DSRs)
- B. Insider risk management policies
- C. Communication compliance policies
- D. Audit log retention policies

**Answer: C**

**NEW QUESTION 65**

- (Exam Topic 5)

You have a Microsoft 365 E5 tenant. Users store data in the following locations:

- > Microsoft Teams
- > Microsoft OneDrive
- > Microsoft Exchange Online

> Microsoft SharePoint Online

You need to retain Microsoft 365 data for two years.

What is the minimum number of retention policies that you should create?

- A. 1
- B. 2
- C. 3
- D. 4

**Answer: C**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-retention-policies?view=o365-worldwide>

**NEW QUESTION 70**

- (Exam Topic 5)

You are reviewing alerts in the Microsoft 365 Defender portal.

How long are the alerts retained in the portal?

- A. 30 days
- B. 60 days
- C. 3 months
- D. 6 months
- E. 12 months

**Answer: C**

**Explanation:**

Data retention information for Microsoft Defender for Office 365

By default, data across different features is retained for a maximum of 30 days. However, for some of the features, you can specify the retention period based on policy. See the following table for the different retention periods for each feature.

Defender for Office 365 Plan 1

\* Alert metadata details (Microsoft Defender for Office alerts) 90 days.

Note: By default, the alerts queue in the Microsoft 365 Defender portal displays the new and in progress alerts from the last 30 days. The most recent alert is at the top of the list so you can see it first.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/mdo-data-retention>

**NEW QUESTION 73**

- (Exam Topic 5)

You have several devices enrolled in Microsoft Endpoint Manager

You have a Microsoft Azure Active Directory (Azure AD) tenant that includes the users shown in the following table.

Name	Role	Member of
User1	Cloud device administrator	GroupA
User2	Intune administrator	GroupB
User3	None	None

The device limit restrictions in Endpoint manager are configured as shown in the following table.

Priority	Name	Device limit	Assigned to
1	Policy1	15	GroupB
2	Policy2	10	GroupA
Default	All users	5	All users

You add user as a device enrollment manager in Endpoint manager

For each of the following statements, select Yes if the statement is true. Otherwise, select No

Answer Area

Statements	Yes	No
User1 can enroll a maximum of 10 devices in Endpoint Manager.	<input type="radio"/>	<input type="radio"/>
User2 can enroll a maximum of 10 devices in Endpoint Manager.	<input type="radio"/>	<input type="radio"/>
User3 can enroll an unlimited number of devices in Endpoint Manager.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Answer Area

Statements	Yes	No
User1 can enroll a maximum of 10 devices in Endpoint Manager.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can enroll a maximum of 10 devices in Endpoint Manager.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can enroll an unlimited number of devices in Endpoint Manager.	<input checked="" type="radio"/>	<input type="radio"/>

**NEW QUESTION 78**

- (Exam Topic 5)

You have a Microsoft 365 subscription.

You need to create a data loss prevention (DLP) policy that is configured to use the Set headers action. To which location can the policy be applied?

- A. OneDrive accounts
- B. Exchange email
- C. Teams chat and channel messages
- D. SharePoint sites

**Answer: B**

**NEW QUESTION 79**

- (Exam Topic 5)

Your company has a Microsoft 365 E5 tenant.

Users at the company use the following versions of Microsoft Office:

- Microsoft 365 Apps for enterprise
- Office for the web
- Office 2016
- Office 2019

The company currently uses the following Office file types:

- .docx
- .xlsx
- .doc
- .xls

You plan to use sensitivity labels. You need to identify the following:

- Which versions of Office require an add-in to support the sensitivity labels.
- Which file types support the sensitivity labels.

What should you identify? To answer, select the appropriate options in the answer area, NOTE: Each correct selection is worth one point.

Answer Area

Office versions that require an add-in to support the sensitivity labels:

- Microsoft 365 Apps for enterprise and Office for the web only
- Office 2016 only
- Office 2019 only
- Office for the web only
- Office 2016 and Office 2019 only
- Microsoft 365 Apps for enterprise only
- Microsoft 365 Apps for enterprise and Office for the web only

Office file types that support the sensitivity labels:

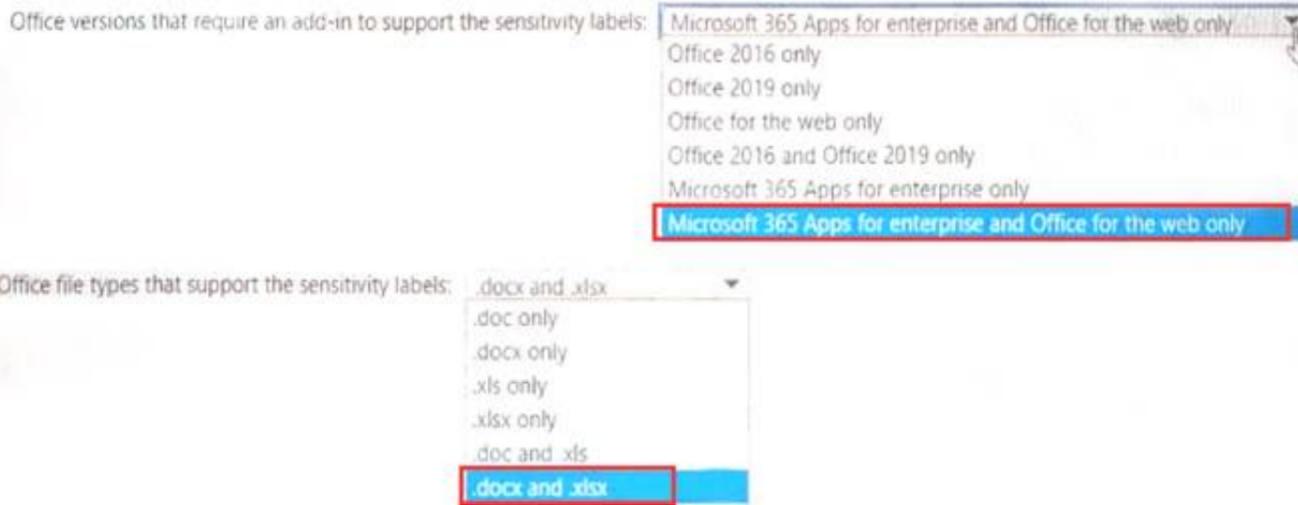
- .docx and .xlsx
- .doc only
- .docx only
- .xls only
- .xlsx only
- .doc and .xls
- .docx and .xlsx

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

**Answer Area**



**NEW QUESTION 83**

- (Exam Topic 5)

Your company has a Microsoft 365 E5 tenant that contains a user named User1. You review the company's compliance score. You need to assign the following improvement action to User1: Enable self-service password reset. What should you do first?

- A. From Compliance Manager, turn off automated testing.
- B. From the Azure Active Directory admin center, enable self-service password reset (SSPR).
- C. From the Microsoft 365 admin center, modify the self-service password reset (SSPR) settings.
- D. From the Azure Active Directory admin center, add User1 to the Compliance administrator role.

**Answer:** D

**Explanation:**

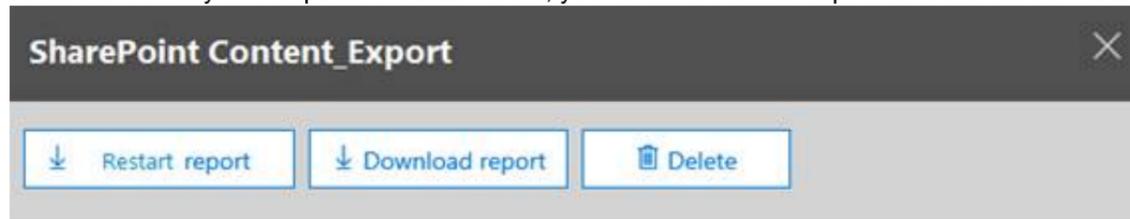
Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-improvement-actions?view=o>  
<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-assign-role-azure-p>

**NEW QUESTION 84**

- (Exam Topic 5)

From the Security & Compliance admin center, you create a content export as shown in the exhibit. (Click the Exhibit tab.)



**Status:**

The export has completed. You can start downloading the results.

**Items included from the search:**

All items, excluding ones that have unrecognized format, are encrypted, or weren't indexed for other reasons.

**Exchange content format:**

One PST file for each mailbox.

**De-duplication for Exchange content:**

Not enabled.

**SharePoint document versions:**

Included

**Export files in a compressed (zipped) folder:**

Yes

**The export data was prepared within region:**

Default region

Close

Feedback

What will be excluded from the export?

- A. a 10-MB XLSX file
- B. a 5-MB MP3 file

- C. a 5-KB RTF file
- D. an 80-MB PPTX file

**Answer: B**

**Explanation:**

Unrecognized file formats are excluded from the search.

Certain types of files, such as Bitmap or MP3 files, don't contain content that can be indexed. As a result, the search indexing servers in Exchange and SharePoint don't perform full-text indexing on these types of files. These types of files are considered to be unsupported file types.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/partially-indexed-items-in-content-search?view=o3> <https://docs.microsoft.com/en-us/office365/securitycompliance/export-a-content-search-report>

**NEW QUESTION 87**

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription.

You plan to implement Microsoft 365 compliance policies to meet the following requirements:

- > Identify documents that are stored in Microsoft Teams and SharePoint Online that contain Personally Identifiable Information (PII).
- > Report on shared documents that contain PII. What should you create?

- A. an alert policy
- B. a data loss prevention (DLP) policy
- C. a retention policy
- D. a Microsoft Cloud App Security policy

**Answer: B**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide>

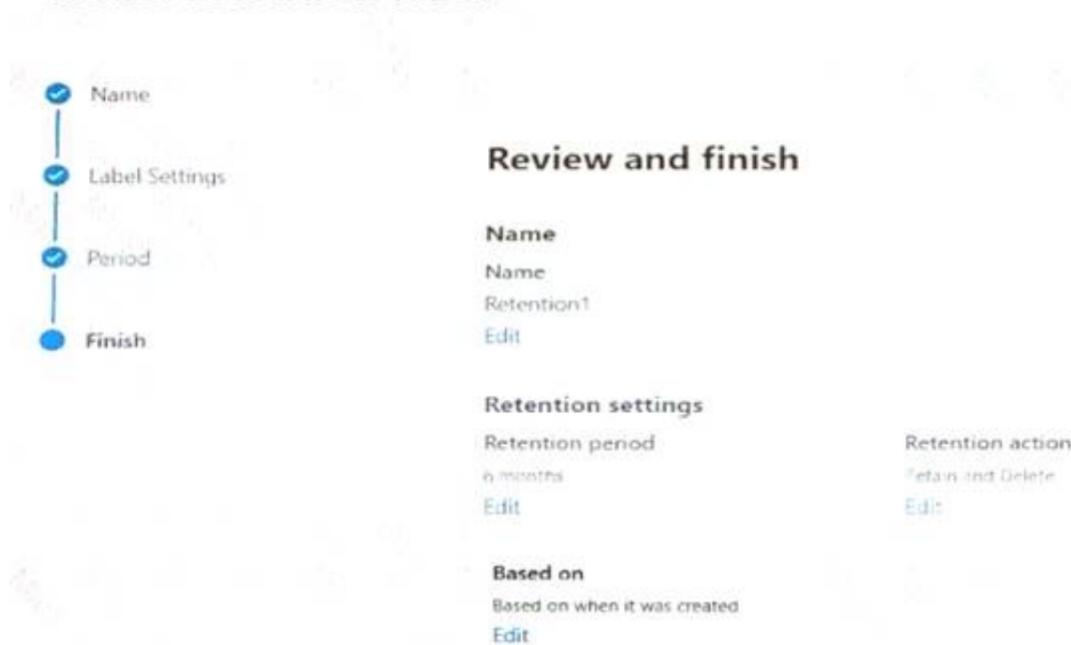
**NEW QUESTION 89**

- (Exam Topic 5)

You have a Microsoft 365 subscription.

You create a retention label named Retention1 as shown in the following exhibit.

**Create retention label**



You apply Retention1 to all the Microsoft OneDrive content.

On January 1, 2020, a user stores a file named File1 in OneDrive. On January 10, 2020, the user modifies File1.

On February 1, 2020, the user deletes File1.

When will File1 be removed permanently and unrecoverable from OneDrive?

- A. February 1, 2020
- B. July 1, 2020
- C. July 10, 2020
- D. August 1, 2020

**Answer: B**

**NEW QUESTION 94**

- (Exam Topic 5)

You have a Microsoft 365 tenant.

You plan to implement Endpoint Protection device configuration profiles. Which platform can you manage by using the profile?

- A. Ubuntu Linux
- B. macOS
- C. iOS
- D. Android

**Answer: B**

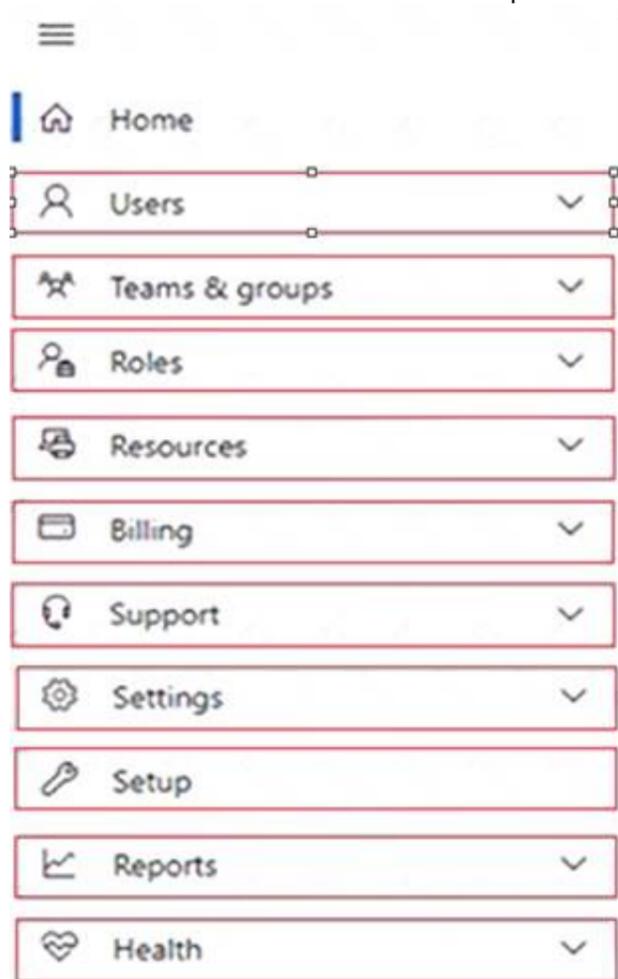
**Explanation:**

Intune device configuration profiles can be applied to Windows 10 devices and macOS devices Note:  
 There are several versions of this question in the exam. The question has two possible correct answers:  
 > Windows 10  
 > macOS  
 Other incorrect answer options you may see on the exam include the following:  
 > Android Enterprise  
 > Windows 8.1 Reference:  
<https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-configure>

**NEW QUESTION 97**

- (Exam Topic 5)  
 HOTSPOT

Your company has a Microsoft 365 E5 subscription. You need to perform the following tasks:  
 View the Adoption Score of the company. Create a new service request to Microsoft.  
 Which two options should you use in the Microsoft 365 admin center? To answer, select the appropriate options in the answer area.  
 NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Box 1: Reports  
 View the Adoption Score of the company. How to enable Adoption Score  
 To enable Adoption Score:  
 > Sign in to the Microsoft 365 admin center as a Global Administrator and go to Reports > Adoption Score  
 > Select enable Adoption Score. It can take up to 24 hours for insights to become available. Box 2: Support  
 Create a new service request to Microsoft.  
 Sign in to Microsoft 365 with your Microsoft 365 admin account, and select Support > New service request. If you're in the admin center, select Support > New service request.  
 Reference:  
<https://learn.microsoft.com/en-us/microsoft-365/admin/adoption/adoption-score> <https://support.microsoft.com/en-us/topic/contact-microsoft-office-support-fd6bb40e-75b7-6f43-d6f9-c13d1085>

**NEW QUESTION 102**

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription that has published sensitivity labels shown in the following exhibit.

Home > sensitivity

**Labels**      Label policies      Auto-labeling(preview)

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. [Learn more about sensitivity labels](#)

+ Create a label    Publish labels    Refresh

Name	Order	Created by	Last modified
Label1	0-highest	Prvi	04/24/2020
- Label2	1	Prvi	04/24/2020
Label3	0-highest	Prvi	04/24/2020
Label4	0-highest	Prvi	04/24/2020
- Label5	5	Prvi	04/24/2020
Label6	0-highest	Prvi	04/24/2020

Which labels can users apply to content?

- A. Label1, Label2, and Label5 only
- B. Label3, Label4, and Label6 only
- C. Label1, Label3, Label2, and Label6 only
- D. Label1, Label2, Label3, Label4, Label5, and Label6

**Answer: C**

**NEW QUESTION 104**

- (Exam Topic 5)

You have a Microsoft 365 E5 tenant.

You configure a device compliance policy as shown in the following exhibit.

**Compliance settings** [Edit](#)

**Microsoft Defender ATP**

Require the device to be at or under the machine risk score.      **Low**

**Device Health**

Rooted devices  
 Require the device to be at or under the Device Threat Level.      **Block**

**System Security**

Require a password to unlock mobile devices      **Require**  
 Required password type      **Device default**  
 Encryption of data storage on device      **Require**  
 Block apps from unknown sources      **Block**

**Actions for noncompliance** [Edit](#)

Action	Schedule
Mark device noncompliant	Immediately
Retire the noncompliant device	Immediately

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

When a device reports a medium threat level, the device will  ▼

be locked remotely

display a notification

marked as compliant

marked as noncompliant

removed from the database

Rooted devices will be  ▼

allowed to access company resources

marked as compliant

prevented from accessing company resources

reported with a low device threat

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, text, application, email Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-android>

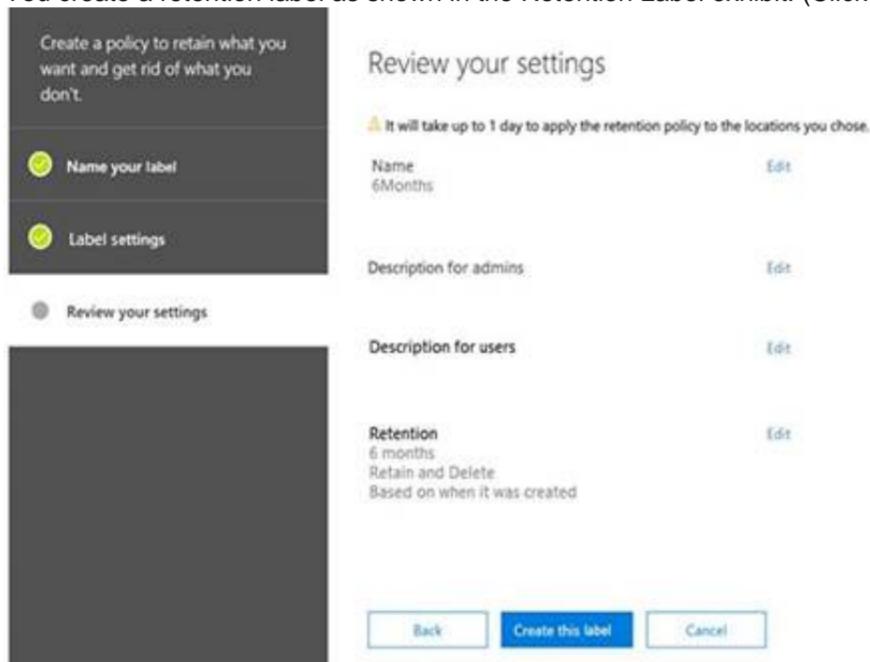
**NEW QUESTION 106**

- (Exam Topic 5)

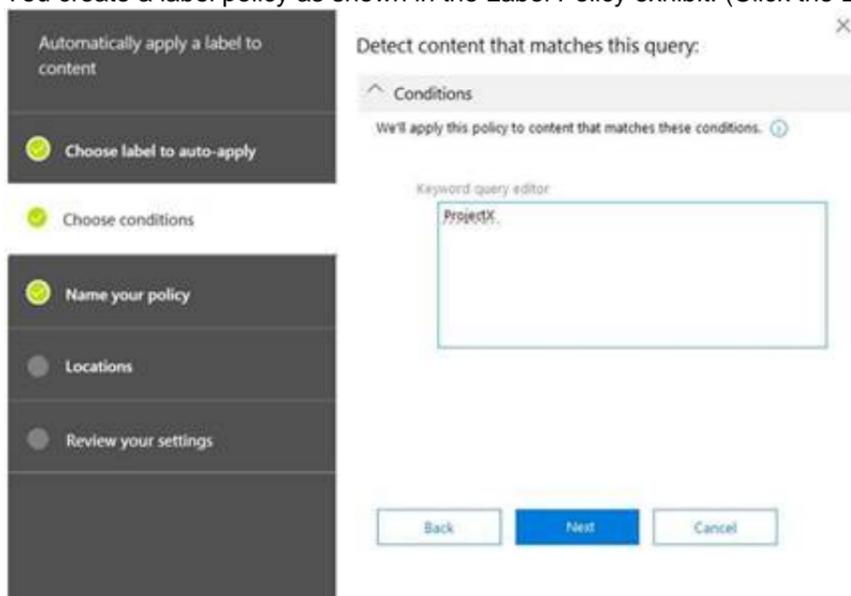
HOTSPOT

You have a Microsoft 365 tenant.

You create a retention label as shown in the Retention Label exhibit. (Click the Retention Label tab.)



You create a label policy as shown in the Label Policy exhibit. (Click the Label Policy tab.)



The label policy is configured as shown in the following table.

Configuration	Value
Label to auto-apply	6Months
Locations	Exchange email

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

**Answer Area**

Statements	Yes	No
Any sent email message that contains the word ProjectX will be deleted immediately.	<input type="radio"/>	<input type="radio"/>
Any sent email message that contains the word ProjectX will be retained for six months.	<input type="radio"/>	<input type="radio"/>
Users are required to manually apply a label to email messages that contain the word ProjectX.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: No

Box 2: Yes

Box 3: No Reference:  
<https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies>

**NEW QUESTION 110**

- (Exam Topic 5)

You configure a data loss prevention (DLP) policy named DLP1 as shown in the following exhibit.

**Choose the types of content to protect**

This policy will protect that matches these requirements. You can choose sensitive info types and existing labels

**Content contains**

Any of these ▾

Sensitive info type	Match accuracy		
	min	max	
Credit Card Number	85	100	x

**Retention labels**

1 year x

Add ▾

[+ Add group](#)

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.  
 NOTE: Each correct selection is worth one point.

DLP1 cannot be applied to [answer choice].

▼

Exchange email

SharePoint sites

OneDrive accounts

DLP1 will be applied only to documents that have [answer choice].

▼

both a credit card number and the 1 year label applied

either a credit card number or the 1 year label applied

between 85 and 100 credit card numbers

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Using a retention label in a policy is only supported for items in SharePoint Online and OneDrive for Business.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwid>

**NEW QUESTION 114**

- (Exam Topic 5)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

The domain syncs to an Azure AD tenant named contoso.com as shown in the exhibit. (Click the Exhibit tab.)

**PROVISION FROM ACTIVE DIRECTORY**



**Azure AD Connect cloud provisioning**

This feature allows you to manage provisioning from the cloud.

[Manage provisioning \(Preview\)](#)

**Azure AD Connect sync**

Sync Status	Enabled
Last Sync	Less than 1 hour ago
Password Hash Sync	Enabled

**USER SIGN-IN**



Federation	Disabled	0 domains
Seamless single sign-on	Enabled	1 domain
Pass-through authentication	Enabled	2 agents

User2 fails to authenticate to Azure AD when signing in as user2@fabrikam.com. You need to ensure that User2 can access the resources in Azure AD. Solution: From the Microsoft Entra admin center, you add fabrikam.com as a custom domain. You instruct User2 to sign in as user2@fabrikam.com. Does this meet the goal?

- A. Yes
- B. No

**Answer:** A

**Explanation:**

The on-premises Active Directory domain is named contoso.com. To enable users to sign on using a different UPN (different domain), you need to add the domain to Microsoft 365 as a custom domain.

**NEW QUESTION 117**

- (Exam Topic 5)

HOTSPOT

You have a Microsoft 365 E5 subscription linked to an Azure Active Directory (Azure AD) tenant. The tenant contains a group named Group1 and the users shown in the following table:

Name	Role
Admin1	Conditional Access administrator
Admin2	Security administrator
Admin3	User administrator

The tenant has a conditional access policy that has the following configurations: Name: Policy1

Assignments:

- Users and groups: Group1
- Cloud apps or actions: All cloud apps
- > Access controls:
  - > Grant, require multi-factor authentication
  - > Enable policy: Report-only

You set Enabled Security defaults to Yes for the tenant.

For each of the following settings select Yes, if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Statements	Yes	No
Admin1 can set Enable policy for Policy1 to <b>On</b> .	<input type="radio"/>	<input type="radio"/>
Admin2 can set Enable policy for Policy1 to <b>Off</b> .	<input type="radio"/>	<input type="radio"/>
Admin3 can set Users and groups for Policy1 to <b>All users</b> .	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Report-only mode is a new Conditional Access policy state that allows administrators to evaluate the impact of Conditional Access policies before enabling them in their environment. With the release of report-only mode:

- > Conditional Access policies can be enabled in report-only mode.
- > During sign-in, policies in report-only mode are evaluated but not enforced.
- > Results are logged in the Conditional Access and Report-only tabs of the Sign-in log details.
- > Customers with an Azure Monitor subscription can monitor the impact of their Conditional Access policies using the Conditional Access insights workbook.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-report-on>

**NEW QUESTION 122**

- (Exam Topic 5)

HOTSPOT

You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

Name	Role
User1	Global admin
User2	None
User3	None

You provision the private store in Microsoft Store for Business.

You assign Microsoft Store for Business roles to the users as shown in the following table.

Name	Role
User1	None
User2	Purchaser
User3	Basic Purchaser

You need to identify which users can add apps to the private store, and which users can assign apps from Microsoft Store for Business. Which users should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Can add apps to the private store:

	▼
User2 only	
User1 and User2 only	
User2 and User3 only	
User1, User2, and User3	

Can assign apps from Microsoft Store for Business:

	▼
User2 only	
User1 and User2 only	
User2 and User3 only	
User1, User2, and User3	

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, text, application Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for-business> <https://docs.microsoft.com/en-us/education/windows/education-scenarios-store-for-business#basic-purchaser-rol>

**NEW QUESTION 127**

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription.

You define a retention label that has the following settings:

- Retention period 7 years
- Start the retention period based on: When items were created

You need to prevent the removal of the label once the label is applied to a file. What should you select in the retention label settings?

- A. Retain items even if users delete
- B. Mark items as a record
- C. Mark items as a regulatory record
- D. Retain items forever

**Answer:** B

**NEW QUESTION 131**

- (Exam Topic 5)

You have a Microsoft 365 tenant that contains devices enrolled in Microsoft Intune. The devices are configured as shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android
Device3	iOS

You plan to perform the following device management tasks in Microsoft Endpoint Manager:

- > Deploy a VPN connection by using a VPN device configuration profile.
- > Configure security settings by using an Endpoint Protection device configuration profile. You support the management tasks.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

VPN device configuration profile:

	▼
Device1 only	
Device1 and Device2 only	
Device1 and Device3 only	
Device1, Device2 and Device3	

Endpoint Protection device configuration profile:

	▼
Device1 only	
Device1 and Device2 only	
Device1 and Device3 only	
Device1, Device2 and Device3	

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, application Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/mem/intune/configuration/vpn-settings-configure> <https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-macos>

**NEW QUESTION 134**

- (Exam Topic 5)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 E5 subscription.

You create an account for a new security administrator named SecAdmin1.

You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.

Solution: From the Microsoft Entra admin center, you assign SecAdmin1 the Security Administrator role.

Does this meet the goal?

- A. Yes
- B. No

**Answer: A**

**Explanation:**

You need to assign the Security Administrator role. Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp>

**NEW QUESTION 139**

- (Exam Topic 5)

You have a Microsoft 365 subscription that contains a user named User1. User1 requires admin access to perform the following tasks:

Manage Microsoft Exchange Online settings.

Create Microsoft 365 groups.

You need to ensure that User1 only has admin access for eight hours and requires approval before the role assignment takes place.

What should you use?

- A. Azure AD Identity Protection
- B. Microsoft Entra Verified ID
- C. Conditional Access
- D. Azure AD Privileged Identity Management (PIM)

**Answer: D**

**Explanation:**

Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about. Here are some of the key features of Privileged Identity Management:

Provide just-in-time privileged access to Azure AD and Azure resources Assign time-bound access to resources using start and end dates Require approval to activate privileged roles

Enforce multi-factor authentication to activate any role Use justification to understand why users activate

Get notifications when privileged roles are activated Conduct access reviews to ensure users still need roles Download audit history for internal or external audit

Prevents removal of the last active Global Administrator and Privileged Role Administrator role assignments. Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

**NEW QUESTION 140**

- (Exam Topic 5)

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the objects shown in the following table.

Name	Configuration
Group1	Global security group
User1	Enabled user account
User2	Disabled user account

You configure Azure AD Connect to sync contoso.com to Azure AD. Which objects will sync to Azure AD?

- A. Group1 only
- B. User1 and User2 only
- C. Group1 and User1 only
- D. Group1, User1, and User2

**Answer: D**

**Explanation:**

Disabled accounts

Disabled accounts are synchronized as well to Azure AD. Disabled accounts are common to represent resources in Exchange, for example conference rooms. The exception is users with a linked mailbox; as previously mentioned, these will never provision an account to Azure AD.

The assumption is that if a disabled user account is found, then we won't find another active account later and the object is provisioned to Azure AD with the userPrincipalName and sourceAnchor found. In case another active account will join to the same metaverse object, then its userPrincipalName and sourceAnchor will be used.

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/concept-azure-ad-connect-sync-user-and>

**NEW QUESTION 142**

- (Exam Topic 5)

You have a Microsoft 365 subscription.

Your company has a customer ID associated to each customer. The customer IDs contain 10 numbers followed by 10 characters. The following is a sample customer ID: 12-456-7890-abc-de-fghij.

You plan to create a data loss prevention (DLP) policy that will detect messages containing customer IDs. D18912E1457D5D1DDCDBD40AB3BF70D5D

What should you create to ensure that the DLP policy can detect the customer IDs?

- A. a sensitive information type
- B. a sensitivity label
- C. a supervision policy
- D. a retention label

**Answer: A**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/custom-sensitive-info-types?view=o365-worldwide>

**NEW QUESTION 144**

- (Exam Topic 5)

You have a Microsoft 365 tenant that has Enable Security defaults set to No in Azure Active Directory (Azure AD).

The tenant has two Compliance Manager assessments as shown in the following table.

Name	Score	Status	Assessment progress	Your improvement actions	Microsoft actions	Group	Product	Regulation
SP800	15444	Incomplete	72%	3 of 450 completed	887 of 887 completed	Group1	Microsoft 365	NIST 800-53
Data Protection Baseline	14370	Incomplete	70%	3 of 489 completed	835 of 835 completed	Group2	Microsoft 365	Data Protection Baseline

The SP800 assessment has the improvement actions shown in the following table.

Improvement action	Test status	Impact	Points achieved	Regulations
Establish a threat intelligence program	None	+9 points	0/9	NIST 800-53, Data Protection Baseline
Establish and document a configuration management program	None	+9 points	0/9	NIST 800-53, Data Protection Baseline

You perform the following actions:

> For the Data Protection Baseline assessment, change the Test status of Establish a threat intelligence program to Implemented.

> Enable multi-factor authentication (MFA) for all users.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in the SP800 assessment.	<input type="radio"/>	<input type="radio"/>
The SP800 assessment score will increase by 54 points.	<input type="radio"/>	<input type="radio"/>
The Data Protection Baseline score will increase by 9 points.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Graphical user interface, text Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-assessments?view=o365-worl> <https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score-calculation?view=o365-worldwid>

**NEW QUESTION 149**

- (Exam Topic 5)

You have a Microsoft 365 tenant.

You plan to implement device configuration profiles in Microsoft Intune. Which platform can you manage by using the profiles?

- A. Ubuntu Linux
- B. macOS
- C. Android Enterprise
- D. Windows 8.1

**Answer: D**

**NEW QUESTION 150**

- (Exam Topic 5)

You have a Microsoft Azure Active Directory (Azure AD) tenant named Contoso.com. You create a Microsoft Defender for identity instance Contoso. The tenant contains the users shown in the following table.

Name	Member of group	Azure AD role
User1	Defender for Identity Contoso Administrators	None
User2	Defender for Identity Contoso Users	None
User3	None	Security administrator
User4	Defender for Identity Contoso Users	Global administrator

You need to modify the configuration of the Defender for identify sensors.

Solutions: You instruct User4 to modify the Defender for identity sensor configuration. Does this meet the goal?

- A. Yes
- B. No

**Answer:** A

**NEW QUESTION 154**

- (Exam Topic 5)

**HOTSPOT**

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Role
User1	Global Administrator
User2	Service Support Administrator
User3	Cloud Application Administrator
User4	None

You plan to provide User4 with early access to Microsoft 365 feature and service updates.

You need to identify which Microsoft 365 setting must be configured, and which user can modify the setting. The solution must use the principle of least privilege.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Microsoft 365 setting:

▼

Office installation options

Privileged access

Release preferences

User:

▼

User1 only

User2 only

User3 only

User1 and User2 only

User1 and User3 only

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

Microsoft 365 setting:

User:

**NEW QUESTION 155**

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription.

You plan to implement Microsoft Purview policies to meet the following requirements:

Identify documents that are stored in Microsoft Teams and SharePoint that contain Personally Identifiable Information (PII). Report on shared documents that contain PII. What should you create?

- A. a data loss prevention (DLP) policy
- B. a retention policy
- C. an alert policy
- D. a Microsoft Defender for Cloud Apps policy

**Answer:** A

**Explanation:**

Demonstrate data protection

Protection of personal information in Microsoft 365 includes using data loss prevention (DLP) capabilities. With DLP policies, you can automatically protect sensitive information across Microsoft 365.

There are multiple ways you can apply the protection. Educating and raising awareness to where EU resident data is stored in your environment and how your employees are permitted to handle it represents one level of information protection using Office 365 DLP.

In this phase, you create a new DLP policy and demonstrate how it gets applied to the IBANs.docx file you stored in SharePoint Online in Phase 2 and when you attempt to send an email containing IBANs.

- > From the Security & Compliance tab of your browser, click Home.
- > Click Data loss prevention > Policy.
- > Click + Create a policy.
- > In Start with a template or create a custom policy, click Custom > Custom policy > Next.
- > In Name your policy, provide the following details and then click Next: a. Name: EU Citizen PII Policy
- b. Description: Protect the personally identifiable information of European citizens
- > Etc. Reference:

<https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-discovery-protection-reporting-in-office365-dev-t>

**NEW QUESTION 159**

- (Exam Topic 5)

You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Member of	Azure Active Directory (Azure AD) role
User1	Group1	Global administrator
User2	Group2	Cloud device administrator

You configure an Enrollment Status Page profile as shown in the following exhibit.

## Settings

The enrollment status page appears during initial device setup. If enabled, users can see the installation progress of assigned apps and profiles.

Show app and profile installation progress. Yes  No

Show time limit error when installation takes longer than specified number of minutes.

Show custom message when time limit error occurs. Yes  No

Allow users to collect logs about installation errors. Yes  No

Only show page to devices provisioned by out-of-box experience (OOBE) Yes  No

Block device use until all apps and profiles are installed Yes  No

You assign the policy to Group1.

You purchase the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Statements	Yes	No
If User1 performs the initial device enrollment for Device1, the Enrollment Status Page will show.	<input type="radio"/>	<input type="radio"/>
If User1 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	<input type="radio"/>	<input type="radio"/>
If User2 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-status>

### NEW QUESTION 161

- (Exam Topic 5)

You have a Microsoft 365 subscription.

Your network uses an IP address space of 51.40.15.0/24.

An Exchange Online administrator recently created a role named Role1 from a computer on the network. You need to identify the name of the administrator by using an audit log search.

For which activities should you search and by which field should you filter in the audit log search? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Activities to search for:

▼

Exchange mailbox activities

Site administration activities

Show results for all activities

Role administration activities

Field to filter by:

▼

Item

User

Detail

IP address

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Activities to search for:

- Exchange mailbox activities
- Site administration activities
- Show results for all activities
- Role administration activities

Field to filter by:

- Item
- User
- Detail
- IP address

**NEW QUESTION 163**

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Mailbox size
User1	5 MB
User2	15 MB
User3	25 MB
User4	55 MB

You have a Microsoft Office 365 retention label named Retention1 that is published to Exchange email.

You have a Microsoft Exchange Online retention policy that is applied to all mailboxes. The retention policy contains a retention tag named Retention2.

Which users can assign Retention1 and Retention2 to their emails? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Users who can assign Retention1:

- User4 only
- User3 and User4 only
- User2, User3, and User4 only
- User1, User2, User3, and User4

Users who can assign Retention2:

- User4 only
- User3 and User4 only
- User2, User3, and User4 only
- User1, User2, User3, and User4

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, text, application, chat or text message Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/retention-policies-exchange?view=o365-worldwide>

**NEW QUESTION 165**

- (Exam Topic 5)

You have a Microsoft 365 E5 tenant that has sensitivity label support enabled for Microsoft and SharePoint Online.

You need to enable unified labeling for Microsoft 365 groups. Which cmdlet should you run?

- A. set-unifiedGroup
- B. Set-Labelpolicy
- C. Execute-AzureAdLabelSync
- D. Add-UnifiedGroupLinks

**Answer:** C

**NEW QUESTION 170**

- (Exam Topic 5)

You have a Microsoft 365 tenant that contains a Windows 10 device named Device1 and the Microsoft Endpoint Manager policies shown in the following table.

Name	Type	Block execution of potentially obfuscated scripts (js/vbs/ps)
Policy1	Attack surface reduction (ASR)	Audit mode
Policy2	Microsoft Defender ATP Baseline	Disable
Policy3	Device configuration profile	Not configured

- A. only the settings of Policy1
- B. only the settings of Policy2
- C. only the settings of Policy3
- D. no settings

**Answer: C**

**NEW QUESTION 171**

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.

Platform	Count
Windows 10	50
Android	50
Linux	50

You need to configure an incident email notification rule that will be triggered when an alert occurs only on a Windows 10 device. The solution must minimize administrative effort.

What should you do first?

- A. From the Microsoft 365 admin center, create a mail-enabled security group.
- B. From the Microsoft 365 Defender portal, create a device group.
- C. From the Microsoft Endpoint Manager admin center, create a device category.
- D. From the Azure Active Directory admin center, create a dynamic device group.

**Answer: B**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldw> <https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-email-notifications?view=>

**NEW QUESTION 174**

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription.

You need to create Conditional Access policies to meet the following requirements:

All users must use multi-factor authentication (MFA) when they sign in from outside the corporate network.

Users must only be able to sign in from outside the corporate network if the sign-in originates from a compliant device.

All users must be blocked from signing in from outside the United States and Canada.

Only users in the R&D department must be blocked from signing in from both Android and iOS devices. Only users in the finance department must be able to sign in to an Azure AD enterprise application named

App1. All other users must be blocked from signing in to App1.

What is the minimum number of Conditional Access policies you should create?

- A. 3
- B. 4
- C. 5
- D. 6
- E. 7
- F. 8

**Answer: B**

**Explanation:**

\* Only users in the finance department must be able to sign in to an Azure AD enterprise application named App1. All other users must be blocked from signing in to App1.

One Policy.

\* Only users in the R&D department must be blocked from signing in from both Android and iOS devices. One Policy.

\* Users must only be able to sign in from outside the corporate network if the sign-in originates from a compliant device.

All users must use multi-factor authentication (MFA) when they sign in from outside the corporate network. One policy

\* All users must be blocked from signing in from outside the United States and Canada. Only users in the R&D department must be blocked from signing in from both Android One Policy

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/plan-conditional-access>

**NEW QUESTION 175**

- (Exam Topic 5)

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365. You need to configure policies to meet the following requirements:

- > Customize the common attachments filter.
- > Enable impersonation protection for sender domains.

Which type of policy should you configure for each requirement? To answer, drag the appropriate policy types to the correct requirements. Each policy type may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Policy Types	Answer Area
<input type="checkbox"/> Anti-malware	Customize the common attachments filter: <input type="text"/>
<input type="checkbox"/> Anti-phishing	Enable impersonation protection for sender domains: <input type="text"/>
<input type="checkbox"/> Anti-spam	
<input type="checkbox"/> Safe Attachments	

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

A close-up of a question Description automatically generated

Box 1: Anti-malware

Customize the common attachments filter. See step 5 below.

\* 1. Use the Microsoft 365 Defender portal to create anti-malware policies

In the Microsoft 365 Defender portal at <https://security.microsoft.com>, go to Email & Collaboration > Policies

& Rules > Threat policies > Anti-Malware in the Policies section. To go directly to the Anti-malware page, use <https://security.microsoft.com/antimalwarev2>

\* 2. On the Anti-malware page, select Create to open the new anti-malware policy wizard. On the Name your policy page, configure these settings:

Name: Enter a unique, descriptive name for the policy. Description: Enter an optional description for the policy.

\* 3. When you're finished on the Name your policy page, select Next.

\* 4. On the Users and domains page, identify the internal recipients that the policy applies to (recipient conditions)

\* 5. On the Protection settings page, configure the following settings: Protection settings section:

Enable the common attachments filter: If you select this option, messages with the specified attachments are treated as malware and are automatically quarantined. You can modify the list by clicking Customize file types and selecting or deselecting values in the list.

\* 6. Etc.

Box 2: Anti-phishing

Enable impersonation protection for sender domains. Anti-phishing policies in Microsoft 365

The high-level differences between anti-phishing policies in EOP and anti-phishing policies in Defender for Office 365 are described in the following table:

Feature	Anti-phishing policies in EOP	Anti-phishing policies in Defender for Office 365
Automatically created default policy	✓	✓
Create custom policies	✓	✓
Common policy settings*	✓	✓
Spoof settings	✓	✓
First contact safety tip	✓	✓
Impersonation settings		✓
Advanced phishing thresholds		✓

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-malware-policies-configure> <https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-phishing-policies-about>

**NEW QUESTION 177**

- (Exam Topic 5)

HOTSPOT

You have a Microsoft 365 E5 subscription.

All company-owned Windows 11 devices are onboarded to Microsoft Defender for Endpoint. You need to configure Defender for Endpoint to meet the following requirements:

- > Block a vulnerable app until the app is updated.
- > Block an application executable based on a file hash. The solution must minimize administrative effort.

What should you configure for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Block a vulnerable app until the app is updated:

▼

An allow or block file

A file indicator

A remediation request

An update ring

Block an application executable based on a file hash:

▼

An allow or block file

A file indicator

A remediation request

An update ring

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Box 1: A remediation request

Block a vulnerable app until the app is updated. Block vulnerable applications

How to block vulnerable applications

- > Go to Vulnerability management > Recommendations in the Microsoft 365 Defender portal.
- > Select a security recommendation to see a flyout with more information.
- > Select Request remediation.
- > Select whether you want to apply the remediation and mitigation to all device groups or only a few.
- > Select the remediation options on the Remediation request page. The remediation options are software update, software uninstall, and attention required.
- > Pick a Remediation due date and select Next.
- > Under Mitigation action, select Block or Warn. Once you submit a mitigation action, it is immediately applied.
- > Review the selections you made and Submit request. On the final page you can choose to go directly to the remediation page to view the progress of remediation activities and see the list of blocked applications.

Box 2: A file indicator

Block an application executable based on a file hash.

While taking the remediation steps suggested by a security recommendation, security admins with the proper permissions can perform a mitigation action and block vulnerable versions of an application. File indicators of compromise (IOC)s are created for each of the executable files that belong to vulnerable versions of that application. Microsoft Defender Antivirus then enforces blocks on the devices that are in the specified scope.

The option to View details of blocked versions in the Indicator page brings you to the Settings > Endpoints > Indicators page where you can view the file hashes and response actions.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-vulnerability-management/tvm-block-vuln-ap>

**NEW QUESTION 179**

- (Exam Topic 5)

You have a Microsoft 365 subscription.

You need to configure a compliance solution that meets the following requirements: Defines sensitive data based on existing data samples

Automatically prevents data that matches the samples from being shared externally in Microsoft SharePoint or email messages

Which two components should you configure? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. a trainable classifier
- B. a sensitive info type
- C. an insider risk policy
- D. an adaptive policy scope
- E. a data loss prevention (DLP) policy

**Answer: AE**

**Explanation:**

A: Classifiers

This categorization method is well suited to content that isn't easily identified by either the manual or automated pattern-matching methods. This method of categorization is more about using a classifier to identify an item based on what the item is, not by elements that are in the item (pattern matching). A classifier learns how to identify a type of content by looking at hundreds of examples of the content you're interested in identifying.

Where you can use classifiers

Classifiers are available to use as a condition for: Office auto-labeling with sensitivity labels

Auto-apply retention label policy based on a condition Communication compliance

Sensitivity labels can use classifiers as conditions, see Apply a sensitivity label to content automatically. Data loss prevention

E: Organizations have sensitive information under their control such as financial data, proprietary data, credit card numbers, health records, or social security numbers. To help protect this sensitive data and reduce risk, they need a way to prevent their users from inappropriately sharing it with people who shouldn't have it. This practice is called data loss prevention (DLP).

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/compliance/classifier-learn-about> <https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp>

**NEW QUESTION 183**

- (Exam Topic 5)

You have a Microsoft 365 subscription that uses an Azure AD tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Role
User1	Exchange Administrator
User2	User Administrator
User3	Global Administrator
User4	None

You add another user named User5 to the User Administrator role. You need to identify which two management tasks User5 can perform. Which two tasks should you identify? Each correct answer presents a complete solution.  
 NOTE: Each correct selection is worth one point.

- A. Delete User2 and User4 only.
- B. Reset the password of User4 only
- C. Reset the password of any user in Azure AD.
- D. Delete User1, User2, and User4 only.
- E. Reset the password of User2 and User4 only.
- F. Delete any user in Azure AD.

**Answer:** AE

**Explanation:**

Users with the User Administrator role can create users and manage all aspects of users with some restrictions (see below). Only on users who are non-admins or in any of the following limited admin roles:

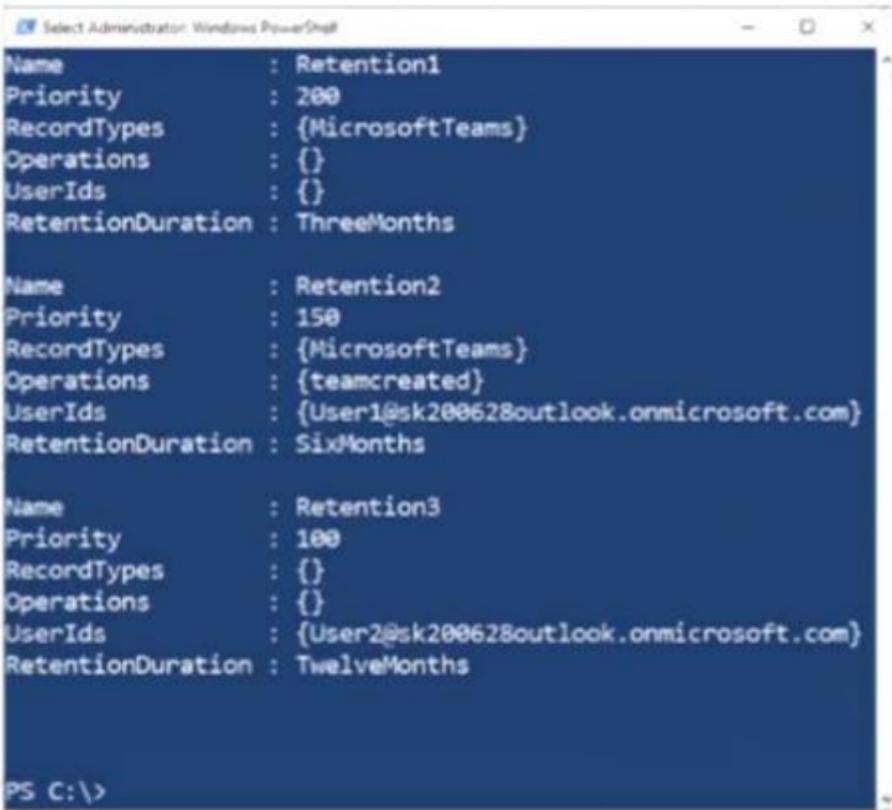
- Directory Readers
- Guest Inviter
- Helpdesk Administrator
- Message Center Reader
- Reports Reader
- User Administrator Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles#availab>

**NEW QUESTION 184**

- (Exam Topic 5)

You have a Microsoft 365 ES subscription that has three auto retention policies as show in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic NOTE Each correct selection is worth one point.

Answer Area

If User1 creates a team in Microsoft Teams, the event is [answer choice]

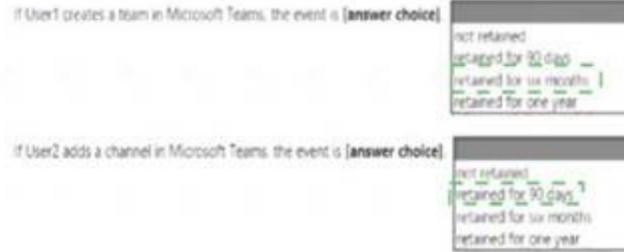
If User2 adds a channel in Microsoft Teams, the event is [answer choice]

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Answer Area



**NEW QUESTION 188**

- (Exam Topic 5)

You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Department
User1	Human resources
User2	Research
User3	Human resources
User4	Marketing

You need to configure group-based licensing to meet the following requirements:

- > To all users, deploy an Office 365 E3 license without the Power Automate license option.
- > To all users, deploy an Enterprise Mobility + Security E5 license.
- > To the users in the research department only, deploy a Power BI Pro license.
- > To the users in the marketing department only, deploy a Visio Plan 2 license.

What is the minimum number of deployment groups required?

- A. 1
- B. 2
- C. 3
- D. 4
- E. 5

**Answer: C**

**Explanation:**

One for all users, one for the research department, and one for the marketing department. Note: What are Deployment Groups?

With Deployment Groups, you can orchestrate deployments across multiple servers and perform rolling updates, while ensuring high availability of your application throughout. You can also deploy to servers

on-premises or virtual machines on Azure or any cloud, plus have end-to-end traceability of deployed artifact versions down to the server level.

Reference:

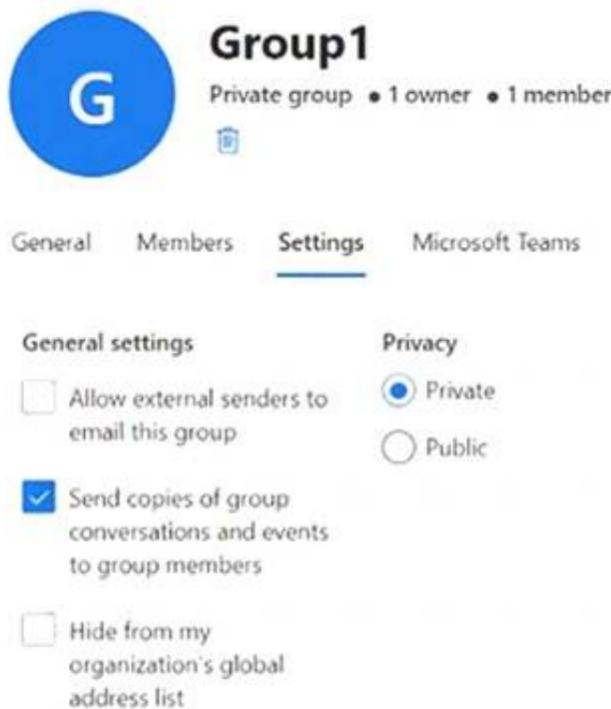
<https://devblogs.microsoft.com/devops/deployment-groups-is-now-generally-available-sharing-of-targets-and-m>

**NEW QUESTION 190**

- (Exam Topic 5)

HOTSPOT

You have a Microsoft 365 subscription that contains a Microsoft 365 group named Group1. Group1 is configured as shown in the following exhibit.



An external user named User1 has an email address of user1@outlook.com. You need to add User1 to Group1.

What should you do first, and which portal should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Action:

- Add User1 to the subscription as an active user.
- For Group1, change the Privacy setting to Public.
- For Group1, select Allow external senders to email this group.
- Invite User1 to collaborate with your organization as a guest.

Portal:

- The Microsoft Entra admin center
- The Exchange admin center
- The Microsoft 365 admin center
- The Microsoft Purview compliance portal

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Invite User1 to collaborate with your organization as a guest.

To manage guest users of a Microsoft 365 tenant via the Admin Center portal, go through the following steps. Navigate with your Web browser to <https://admin.microsoft.com>.

On the left pane, click on "Users", then click "Guest Users".

On the "Guest Users" page, to create a new guest user, click on either the "Add a guest user" link on the top of the page or click on "Go to Azure Active Directory to add guest users" link at the bottom of the page. Both of these links will take you to the Azure Active Directory portal, which is located at <https://aad.portal.azure.com>.

On the "New user" page in the Microsoft Azure portal, you must choose to either "Create user" or "Invite user". If you choose the "Create user" option, this will create a new user in your organization, which will have a login address with format username@tenantdomain.dot.com. If you choose the "Invite user" option, this will invite a new guest user to collaborate with your organization. The user will be emailed an email invitation which they can accept in order to begin collaborating. For the purpose of creating a guest user, you must choose the "Invite user" option.

Box 2: The Microsoft Entra admin center

Microsoft Entra admin center unites Azure AD with family of identity and access products

Microsoft Entra admin center gives customers an entire toolset to secure access for everyone and everything in multicloud and multiplatform environments. The entire Microsoft Entra product family is available at this new admin center, including Azure Active Directory (Azure AD) and Microsoft Entra Permissions Management, formerly known as CloudKnox.

Starting this month, waves of customers will begin to be automatically directed to [entra.microsoft.com](https://entra.microsoft.com) from Microsoft 365 in place of the Azure AD admin center ([aad.portal.azure.com](https://aad.portal.azure.com)).

Reference:

<https://stefanos.cloud/kb/how-to-manage-microsoft-365-guest-users> <https://m365admin.handsontek.net/microsoft-entra-admin-center-unites-azure-ad-with-family-of-identity-and-ac>

**NEW QUESTION 193**

- (Exam Topic 5)

You have a Microsoft 365 E5 tenant that contains 100 Windows 10 devices.

You plan to deploy a Windows 10 Security Baseline profile that will protect secrets stored in memory. What should you configure in the profile?

- A. Microsoft Defender Credential Guard
- B. BitLocker Drive Encryption (BitLocker)
- C. Microsoft Defender
- D. Microsoft Defender Exploit Guard

**Answer:** A

**NEW QUESTION 197**

- (Exam Topic 5)

You have a Microsoft 365 subscription.

You have the retention policies shown in the following table.

Name	Location	Retain items for a specific period	Start the retention period based on	At the end of the retention period
Policy1	SharePoint sites	1 years	When items were created	Delete items automatically
Policy2	SharePoint sites	2 years	When items were last modified	Do nothing

Both policies are applied to a Microsoft SharePoint site named Site1 that contains a file named File1.docx. File1.docx was created on January 1, 2022 and last modified on January 31,2022. The file was NOT modified again.

When will File1.docx be deleted automatically?

- A. January 1,2023
- B. January 1,2024
- C. January 31, 2023
- D. January 31, 2024
- E. never

**Answer:** D

**Explanation:**

for the four different principles:

\* 1. Retention wins over deletion. Content won't be permanently deleted when it also has retention settings to retain it. While this principle ensures that content is preserved for compliance reasons, the delete process can still be initiated (user-initiated or system-initiated) and consequently, might remove the content from users' main view. However, permanent deletion is suspended.

\* 2. Etc. Reference:

<https://learn.microsoft.com/en-us/microsoft-365/compliance/retention>

**NEW QUESTION 198**

- (Exam Topic 5)

**HOTSPOT**

You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Type	Department
User1	Guest	IT support
User2	Guest	SupportCore
User3	Member	IT support

You need to configure a dynamic user group that will include the guest users in any department that contains the word Support.

How should you complete the membership rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

(user.userType ) and (user.department )

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: -eq "Guest"

Dynamic membership rules for groups in Azure Active Directory Supported expression operators

The following table lists all the supported operators and their syntax for a single expression. Operators can be used with or without the hyphen (-) prefix. The Contains operator does partial string matches but not item in a collection matches.

\* Equals

-eq

\* Contains

-contains

\* Etc.

Box 2: -contains "Support" Incorrect:

\* -in

If you want to compare the value of a user attribute against multiple values, you can use the -in or -notin operators.

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership>

**NEW QUESTION 203**

- (Exam Topic 5)

You have a Microsoft 365 subscription that uses Microsoft Defender for Cloud Apps. You configure a session control policy to block downloads from SharePoint Online sites. Users report that they can still download files from SharePoint Online sites.

You need to ensure that file download is blocked while still allowing users to browse SharePoint Online sites. What should you configure?

- A. an access policy
- B. a data loss prevention (DLP) policy
- C. an activity policy
- D. a Conditional Access policy

**Answer:** A

**NEW QUESTION 208**

- (Exam Topic 5)

You purchase a new computer that has Windows 10, version 2004 preinstalled.

You need to ensure that the computer is up-to-date. The solution must minimize the number of updates installed.

What should you do on the computer?

- A. Install all the feature updates released since version 2004 and all the quality updates released since version 2004 only.
- B. install the West feature update and the latest quality update only.
- C. install all the feature updates released since version 2004 and the latest quality update only.
- D. install the latest feature update and all the quality updates released since version 2004.

**Answer:** B

**NEW QUESTION 211**

- (Exam Topic 5)

You have a Microsoft 365 subscription.

You need to identify which administrative users performed eDiscovery searches during the past week. What should you do from the Security & Compliance admin center?

- A. Perform a content search
- B. Create a supervision policy
- C. Create an eDiscovery case
- D. Perform an audit log search

**Answer: D**

**NEW QUESTION 213**

- (Exam Topic 5)

You have a Microsoft 365 tenant that contains a Windows 10 device. The device is onboarded to Microsoft Defender for Endpoint.

From Microsoft Defender Security Center, you perform a security investigation.

You need to run a PowerShell script on the device to collect forensic information. Which action should you select on the device page?

- A. Initiate Live Response Session
- B. Initiate Automated Investigation
- C. Collect investigation package
- D. Go hunt

**Answer: A**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/live-response?view=o365-worldwid>

**NEW QUESTION 216**

- (Exam Topic 5)

**HOTSPOT**

Your network contains an Active Directory domain named fabrikam.com. The domain contains the objects shown in the following table.

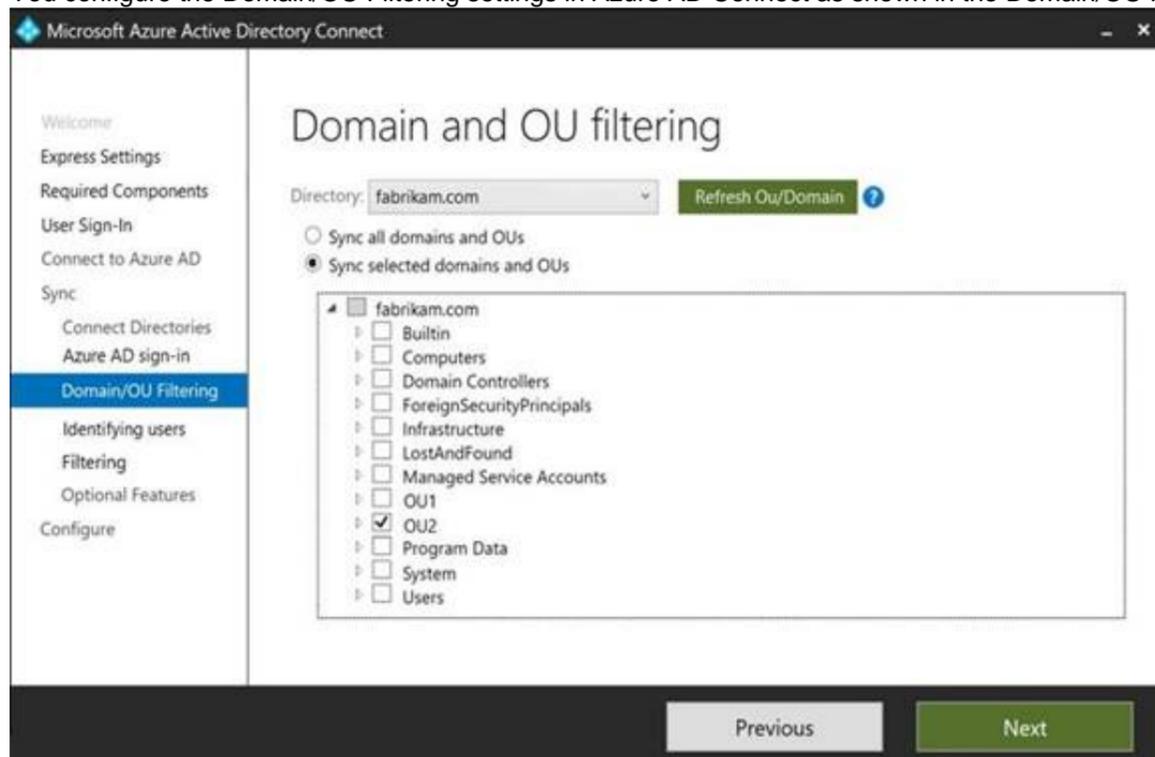
Name	Type	In organizational unit (OU)
User1	User	OU1
User2	User	OU1
Group1	Security Group – Global	OU1
User3	User	OU2
Group2	Security Group – Global	OU2

The groups have the members shown in the following table.

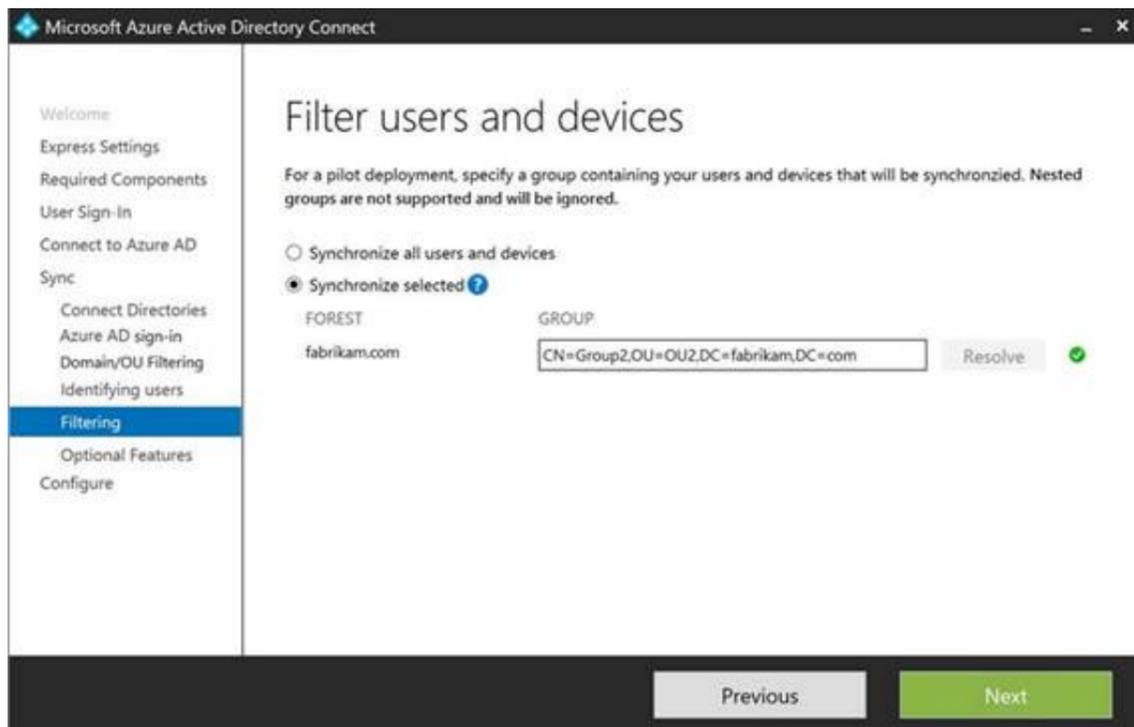
Group	Members
Group1	User1
Group2	User2, User3, Group1

You are configuring synchronization between fabrikam.com and an Azure AD tenant.

You configure the Domain/OU Filtering settings in Azure AD Connect as shown in the Domain/OU Filtering exhibit (Click the Domain/OU Filtering tab.)



You configure the Filtering settings in Azure AD Connect as shown in the Filtering exhibit. (Click the Filtering tab.)



For each of the following statements, select Yes if the statement is true. Otherwise, select No.  
 NOTE: Each correct selection is worth one point.

**Answer Area**

Statements	Yes	No
User2 will synchronize to Azure AD.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Group2 will synchronize to Azure AD.	<input type="checkbox"/>	<input type="checkbox"/>
User3 will synchronize to Azure AD.	<input type="checkbox"/>	<input type="checkbox"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: No

The filtering is configured to synchronize Group2 and OU2 only. The effect of this is that only members of Group2 who are in OU2 will be synchronized.

User2 is in Group2. However, the User2 account object is in OU1 so User2 will not synchronize to Azure AD. Box 2: Yes

Group2 is in OU2 so Group2 will synchronize to Azure AD. However, only members of the group who are in OU2 will synchronize. Members of Group2 who are in OU1 will not synchronize.

Box 3: Yes

User3 is in Group2 and in OU2. Therefore, User3 will synchronize to Azure AD. Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering#group-b>

**NEW QUESTION 221**

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription.

You plan to create a data loss prevention (DLP) policy that will be applied to all available locations. Which conditions can you use in the DLP rules of the policy?

- A. sensitive info types
- B. content search queries
- C. keywords
- D. sensitivity labels

**Answer:** C

**Explanation:**

Apply retention labels to content automatically if it matches specific conditions, that includes cloud attachments that are shared in email or Teams, or when the content contains:

Specific types of sensitive information.

Specific keywords that match a query you create. Pattern matches for a trainable classifier.

Note: Retention policies can be applied to the following locations: Exchange mailboxes

SharePoint classic and communication sites OneDrive accounts

Microsoft 365 Group mailboxes & sites Skype for Business

Exchange public folders

Teams channel messages (standard channels and shared channels)

Teams chats

Teams private channel messages Yammer community messages Yammer user messages Reference:

<https://learn.microsoft.com/en-us/microsoft-365/compliance/retention> <https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-exchange-conditions-and-actions>

**NEW QUESTION 226**

- (Exam Topic 5)

DRAG DROP

You have a Microsoft 365 subscription.

In the Exchange admin center, you have a data loss prevention (DLP) policy named Policy1 that has the following configurations:

- > Block emails that contain financial data.
- > Display the following policy tip text: Message blocked.

From the Security & Compliance admin center, you create a DLP policy named Policy2 that has the following configurations:

- > Use the following location: Exchange email.
- > Display the following policy tip text: Message contains sensitive data.
- > When a user sends an email, notify the user if the email contains health records.

What is the result of the DLP policies when the user sends an email? To answer, drag the appropriate results to the correct scenarios. Each result may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Results	Answer Area
The email will be blocked, and the user will receive the policy tip: Message blocked.	When the user sends an email that contains financial data and health records:
The email will be blocked, and the user will receive the policy tip: Message contains sensitive data.	When the user sends an email that contains only financial data:
The email will be allowed, and the user will receive the policy tip: Message blocked.	
The email will be allowed, and the user will receive the policy tip: Message contains sensitive data.	
The email will be allowed, and a message policy tip will NOT be displayed.	

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Box 1: The email will be blocked, and the user will receive the policy tip: Message blocked.

If you've created DLP policies in the Exchange admin center, those policies will continue to work side by side with any policies for email that you create in the Security & Compliance Center. But note that rules created in the Exchange admin center take precedence. All Exchange mail flow rules are processed first, and then the DLP rules from the Security & Compliance Center are processed.

Box 2: The email will be allowed, and the user will receive the policy tip: Message contains sensitive data. Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/how-dlp-works-between-admin-centers>

**NEW QUESTION 230**

- (Exam Topic 5)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an on-premises Active Directory domain. The domain contains domain controllers that run Windows Server 2019. The functional level of the forest and the domain is Windows Server 2012 R2.

The domain contains 100 computers that run Windows 10 and a member server named Server1 that runs Windows Server 2012 R2.

You plan to use Server1 to manage the domain and to configure Windows 10 Group Policy settings. You install the Group Policy Management Console (GPMC) on Server1.

You need to configure the Windows Update for Business Group Policy settings on Server1. Solution: You upgrade Server1 to Windows Server 2019.

Does this meet the goal?

- A. yes
- B. No

**Answer: A**

**NEW QUESTION 233**

- (Exam Topic 5)

You have a Microsoft 365 E3 subscription that uses Microsoft Defender for Endpoint Plan 1.

Which two Defender for Endpoint features are available to the subscription? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. advanced hunting
- B. security reports
- C. digital certificate assessment
- D. device discovery
- E. attack surface reduction (ASR)

**Answer: BE**

**Explanation:**

B: Overview of Microsoft Defender for Endpoint Plan 1, Reporting

The Microsoft 365 Defender portal (<https://security.microsoft.com>) provides easy access to information about detected threats and actions to address those

threats.  
 The Home page includes cards to show at a glance which users or devices are at risk, how many threats were detected, and what alerts/incidents were created. The Incidents & alerts section lists any incidents that were created as a result of triggered alerts. Alerts and incidents are generated as threats are detected across devices.  
 The Action center lists remediation actions that were taken. For example, if a file is sent to quarantine, or a URL is blocked, each action is listed in the Action center on the History tab.  
 The Reports section includes reports that show threats detected and their status. E: What can you expect from Microsoft Defender for Endpoint P1?  
 Microsoft Defender for Endpoint P1 is focused on prevention/EPP including:  
 Next-generation antimalware that is cloud-based with built-in AI that helps to stop ransomware, known and unknown malware, and other threats in their tracks.  
 (E) Attack surface reduction capabilities that harden the device, prevent zero days, and offer granular control over access and behaviors on the endpoint.  
 Device based conditional access that offers an additional layer of data protection and breach prevention and enables a Zero Trust approach.  
 The below table offers a comparison of capabilities are offered in Plan 1 versus Plan 2.

Capabilities	P1	P2
Unified security tools and centralized management	✓	✓
Next-generation antimalware	✓	✓
Attack surface reduction rules	✓	✓
Device control (e.g.: USB)	✓	✓
Endpoint firewall	✓	✓
Network protection	✓	✓
Web control / category-based URL backing	✓	✓
Device-based conditional access	✓	✓
Controlled folder access	✓	✓
APIs, SIEM connector, custom TI	✓	✓
Application control	✓	✓
Endpoint detection and response		✓
Automated investigation and remediation		✓
Threat and vulnerability management		✓
Threat intelligence (Threat Analytics)		✓
Sandbox (deep analysis)		✓
Microsoft Threat Experts**		✓

\*\*Includes Targeted Attack Notifications (TAN) and Experts On Demand (EOD). Customers must apply for TAN. EOD is available for purchase as an add-on.

Incorrect:  
 Not A: P2 is by far the best fit for enterprises that need an EDR solution including automated investigation and remediation tools, advanced threat prevention and threat and vulnerability management (TVM), and hunting capabilities.  
 Reference:  
<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/defender-endpoint-plan-1> <https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/microsoft-defender-for-endpoint-plan>

**NEW QUESTION 235**

- (Exam Topic 5)

You purchase a new computer that has Windows 10, version 21H1 preinstalled. You need to ensure that the computer is up-to-date. The solution must minimize the number of updates installed. What should you do on the computer?

- A. Install all the feature updates released since version 21H1 and the latest quality update only.
- B. Install the latest feature update and all the quality updates released since version 21H1.
- C. Install the latest feature update and the latest quality update only.
- D. Install all the feature updates released since version 21H1 and all the quality updates released since version 21H1 only.

**Answer: C**

**NEW QUESTION 237**

.....

## **Thank You for Trying Our Product**

### **We offer two products:**

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### **MS-102 Practice Exam Features:**

- \* MS-102 Questions and Answers Updated Frequently
- \* MS-102 Practice Questions Verified by Expert Senior Certified Staff
- \* MS-102 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* MS-102 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The MS-102 Practice Test Here](#)**